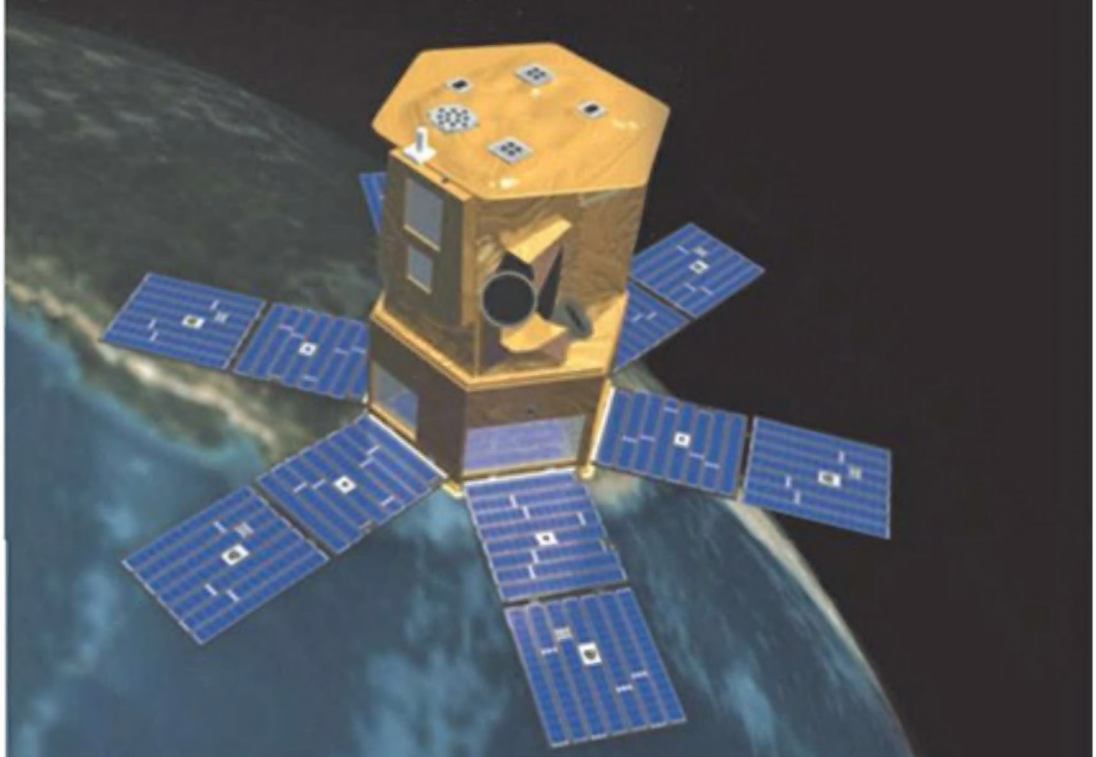
Handbook of Surveillance Technologies

THIRD EDITION



CRC Press
Taylor & Francis Group

J. K. PETERSEN

Copyrighted Material

schemes have two keys, often a *public key* and a *private key* known only to the user. Keys have different lengths which are usually related to the 'strength' of the encryption. Key encryption is one of the most prevalent means of encrypting electronic data for security purposes (compression algorithms also encrypt data, but their primary purpose is not usually to obscure the meaning of the data but rather to store or transmit it more efficiently.)

In general, stronger encryption means longer encryption and/or decryption times, though this is not true in every instance, as more efficient algorithms are sometimes devised. The choice of encryption techniques depends very much on the need for convenience and the required level of security. Personal letters are less sensitive than classified government documents, for example, and function well with lower levels of encryption and single keys (or no keys).

Encryption techniques can be symmetric, in which the encryption and decryption use the same key or in which the encryption and decryption processes require about the same amount of time. They can also be asymmetric, with different keys, or substantially different encryption/decryption times. For purposes of security, a method that is quickly encrypted and slowly decrypted is favored for some purposes. For general correspondence, however, slow decryption is an inconvenience, as are multiple keys.

Encryption systems can be *deterministic* or *nondeterministic*. One that generates the same result each time, given the same key, is deterministic and is generally not as strong as one that generates a different result, given the same key. However, true randomness in computer operations is not usually the rule and many systems are deterministic.

Encryption algorithms can be reversible or irreversible. A reversible scheme is one in which data can be recovered back to its unencrypted state. Irreversible schemes cannot be recovered, but since they tend to be used as authentication or tamper mechanisms rather than as message recovery mechanisms, they are valuable for certain tasks.

Some specific encryption schemes of interest include

- *AES* - IA-8314: Advanced Encryption Standard. A new, stronger encryption algorithm intended by the *National Institute of Standards and Technology* (NIST) Computer Security Division to replace DES. The project was initiated in January 1997 as a standard laboratory network protocol. Da Vinci is an example of a shareware encryption system based upon AES. CipherMax is an example of a commercial product that provides 256-bit AES encryption.
- *APKC (Absolute Public Key Cryptography)* - This system was patented in August 2006. It is a public key cryptographic system and method that offers two-way communication security even when a private key is revealed. APKC can support mobile devices with low processing power and short keys. The keys have two or more components, a random number is bound to each of the components of the public key, the message is encrypted into the same number of cipher versions as components, and the ciphers are delivered to the destination in source routing or hop-by-hop routing with a small time gap. All ciphered version are mathematically manipulated to reconstruct the original message. This method prevents an attack at an intermediary IP router because all cipher versions must be available and the original message cannot be obtained even if the attacker knows the private key. [U.S. Patent # 7088821]
- *Blowfish* - Designed by Bruce Schneier and first presented in 1994. Widespread. Standard in OpenBSD. A symmetric block cipher that accepts a variable-length key from 32 bits up to a maximum of 448 bits. It can be used as a replacement for DES or IDEA. Small block size, good speed, uncomplicated interface. Introduced in *Dr. Dobb's Journal* in Apr. 1994, with source published in *Dr. Dobbs Journal*, Sept. 1995.